TRUSTED COMPUTING ENVIRONMENT

FIELD OF THE INVENTION

The invention relates establishing and/or maintaining a trusted computing environment. A first computing device can be said to regard a second computing device as trustworthy if the first computing device can expect the second computing device to operate or behave in a known manner.

BACKGROUND TO THE INVENTION

In the present context, "trust" and "trusted" are used to mean that a device or service can be relied upon to work in an intended, described or expected manner, and has not been tampered with or subverted in order to run malicious applications. A specification for trusted computing has been developed by the Trusted Computing Platform Alliance and can be found at www.trustedpc.org.

A conventional trusted computing device comprises a tamper resistant tester which can test the device to ascertain if it is trustworthy. The outcome of the test can be used within the device or reported to another computing device attempting to communicate with it. An exemplary trusted component is described in the applicants co-pending International Patent Application Publication No. PCT/GB00/00528 entitled "Trusted Computing Platform", the contents of which are incorporated by reference herein. If the outcome of the test is reported to another device, then that other device can use the report to determine a trust policy vis-a-vis the device offering the report, which controls its communication with the reporting device.

One disadvantage of a computing environment comprised of trusted computing devices of the kind mentioned above arises where a trusted computing device becomes compromised, e.g. by a virus. The trusted computing devices in the environment do not know if the other computing devices within the environment have been compromised unless they challenge

the other computing devices to verify that they have not been compromised. The challenge-verification process can consume undesirable amounts of time and/or processing resources.

SUMMARY OF THE INVENTION

An object of the invention is the amelioration of the aforementioned disadvantage.

According to one aspect, the invention comprises a method of operating a trusted computing system, the method comprising providing an assessor to receive a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report.

According to another aspect, the invention comprises an assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device.

Hence, the invention can provide an efficient way of informing computing devices within an environment about the trustworthiness of other computing devices within the environment, so as to establish or maintain a trusted computing environment. In maintaining a trusted computing environment, the invention may enable a computing device to be sure of, and keep up to date with, the level of trustworthiness of other computing devices in the environment.

In one embodiment, the report contains an assessment of the trustworthiness that has been prepared by the reporting computing device itself. In another embodiment, the report provides information about the reporting computing device that is sufficient to allow the assessor to assess the trustworthiness of the reporting computing device. Preferably, the reporting computing device comprises a trusted component which evaluates the

trustworthiness of the computing device and provides the report. The trusted component is preferably resistant to tampering and capable of applying a digital signature to the report to permit authentication of the report. The reporting computing device may be triggered to provide the report in response to a certain event or any one of a number of predetermined events. For example, the reporting computing device may be triggered to report by a request from an assessor for a trustworthiness report, or by being initialised or reset, or by the occurrence of an undesirable event (e.g. the computing device being compromised by a virus).

The assessor may, subsequent to receiving a trustworthiness report, update the trust policies of more than one computing device, one of which may be the computing device that provided the trustworthiness report.

A computing device in the context of the invention may be, for example, a computer or a peripheral (such as a scanner or printer) or other device having some data processing ability.

BRIEF DESCRIPTION OF THE FIGURES

By way of example only, some embodiments of the invention will now be described by reference to the accompanying drawings in which:

Figure 1 is a block diagram of a trusted computing environment; and

Figure 2 is a block diagram of an assessor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The trusted computing environment 100 of Figure 1 comprises an assessing computer 110, or "assessor", which acts as a service provider to the computing devices in the environment, 112, 114, 116 and 118. In practice, the environment may comprise a different number of computing devices. Each computing device has at least some capacity for processing data and therefore at least some capacity for becoming untrustworthy or

affecting the trustworthiness of other computing devices with which it communicates. In this embodiment, devices 112, 114 and 116 are networked computers and device 118 is a network printer serving devices 112, 114 and 116.

Each of the computing devices 112 to 118 comprises a trusted component and a memory 122 holding a policy. A policy allows a computing device to determine the level to which it trusts other computing devices sharing the environment.

As an example, a policy within a computing device may list the surrounding computing devices and specify the degree to which each of them is to be trusted. In order to set the degree of trust, a policy may specify that a particular computing device is to be interacted with for all purposes, selected purposes or not at all.

As a further example, a policy within a computing device may specify a list of components (either software or hardware) that are untrusted. If a computing device containing such a policy finds one or more of these components in another computing device, then it can determine accordingly the degree to which it trusts that other computing device.

Each trusted component 120 is arranged, in a known manner, to assess the trustworthiness of the computing device with which it is associated, and to report its assessment to the assessor 110. The report may contain, for example, a decision made by the trusted component as to the trustworthiness of its host computing device, or the trusted component may simply audit its host so that the report lists the components of its host. Examples of trusted components, and the monitoring of components or processes of a host, are found in the applicants co-pending International Patent Applications as follows: Publication No. PCT/GB00/02004 entitled "Data Logging in Computing Platform" filed on 25 May 2000 and Publication No. PCT/GB00/00495 entitled "Protection of the Configuration of Modules in Computing Apparatus", filed on 15 February 2000, the contents of which are incorporated by reference.

The trusted component 120 can be arranged to be triggered to report by any of a number of events. For example, the report can be triggered by a request for a report received from the assessor 110, initialisation or resetting of the host computing device, or by some undesirable event (e.g. detection of the computing device being compromised by a known virus or the loading or addition of components unrecognised by the trusted component). Alternatively, the trusted component 120 can be arranged to make periodic reports to the assessor.

To maintain security, the trusted component 120 and the memory 122 holding the policy are incorporated in the corresponding computing device in such a manner that the trusted component 120 can perform its assessments on the computing device and yet the computing device is unable to modify the operation of the trusted component or the content of the policy. The memory 122 is arranged to accept updates to the policy that are certified by containing the digital signature of the assessor 110. Similarly, the trusted component is arranged to certify its outgoing reports with a digital signature which the assessor 110 can verify. The memory 122 containing the policy may be integrated with the trusted component 120.

As shown in Figure 2, the assessor 110 comprises a receiver 200, an updater 210, a transmitter 212 and a requestor 214. In response to being polled by the requestor 214, the receiver 200 receives the reports from the trusted components (which contain, for example, decisions on trustworthiness or component inventories), the updater 210 updates the computing devices' policies as necessary and the transmitter 212 disseminates the updated policies. Clearly it is desirable that the assessor 110 or at least relevant functions thereof are also trusted.

In the present embodiment, the assessor polls the trusted components within the computing devices 112 to 118 for trustworthiness reports. Consider the case where printer 118 has been contaminated by a virus. The report from this device alerts the assessor 110 to this fact and the assessor 110 responds by transmitting updated policies to the computing devices 112 to 118. The extent to which an updated policy curtails the extent to which the

computing device hosting the policy interacts with the affected device 118 depends on the relationship between the two computing devices. In this example, the policy of device 116 is updated to reflect that it can only send urgent print requests to printer 118 and the policies of devices 112 and 114 are updated to reflect that they are not to interact with the printer 118 or, due the continuing potential for it to be compromised by printer 118, computing device 116.

Due to the invention, a trusted computing network or environment can be established or maintained without a computing device being required to directly challenge the trustworthiness of another device when it is required to communicate with that device.